



# Department of Homeland Security Daily Open Source Infrastructure Report for 25 July 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- The Capital–Journal reports that as Topeka, Kansas, sizzled under temperatures topping the century mark, someone stealing copper wire from an electrical substation sparked a power outage that affected about 2,650 homes and businesses. (See item [2](#))
- Both terminals at John Wayne Airport, 35 miles south of Los Angeles, were evacuated Sunday evening, July 23, and passengers were taken off airplanes for re–screening, after a female passenger went past a security checkpoint without being screened. (See item [17](#))
- The Associated Press reports that the FBI has joined the investigation as police combed fields, overpasses, and roads for evidence into the sniper shootings along two Indiana interstates that have killed one person and wounded another. (See item [19](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

1. *July 25, Associated Press* — **Trees pile high as St. Louis awaits return of electricity.** More than 100 dump trucks rolled through city streets Sunday, July 23, collecting mangled trees and branches left behind by last week's powerful storms that cut power to hundreds of thousands of customers. Members of the Missouri Army National Guard are assisting with the cleanup. "It's

hard to believe your eyes when you are looking at something this massive...This is just the beginning," St. Louis Parks Director Gary Bass said. About 290,000 homes and businesses here were still without power Sunday, down from the more than a half-million homes and businesses powerless last week while temperatures soared into triple digits. Four deaths in the region have been attributed to the storms or heat. An AmerenUE utility company spokesperson said it could be at least four days before service is fully restored. The power company has been running television commercials asking for the city's patience and some 4,000 utility workers from as far away as Arizona are restoring power around the clock. President Bush on Friday, July 21, approved Missouri's request for an expedited disaster declaration, which mobilizes the Federal Emergency Management Agency and provides federal funding for debris removal and other emergency needs.

Source: <http://www.belleville.com/mld/belleville/news/state/15106479.htm>

2. *July 25, Capital-Journal (KS)* — **Thieves cause electrical outage.** As Topeka, KS, sizzled Thursday, July 20, under temperatures topping the century mark, officials said someone stealing copper wire from an electrical substation sparked a power outage that affected about 2,650 homes and businesses in North Topeka. Authorities said they seized some of the stolen wire from a scrap yard but hadn't located the person or people responsible for the outage, which cut off power for two hours to Westar Energy customers, including the Topeka Rescue Mission. The power failure was in progress in much of North Topeka when the city's high temperature of 103 and high heat index of 110 for Thursday were recorded. Thursday's theft came at a time when authorities say they are seeing an increase in thefts of copper products. The outage caused traffic signals to stop working at six intersections in North Topeka.

Source: [http://www.cjonline.com/stories/072106/loc\\_outage.shtml](http://www.cjonline.com/stories/072106/loc_outage.shtml)

3. *July 24, Associated Press* — **Phoenix power lines in path of forest wildfire safe.** Crews on Sunday, July 23, kept a wildfire burning in central Arizona from reaching two power lines that send electricity to Phoenix. The lightning-sparked fire was about two miles away from the power lines in the Tonto National Forest, said Paige Rockett, a spokesperson for the U.S. Forest Service. The two lines remained in operation.

Source: <http://www.tucsoncitizen.com/daily/local/20065.php>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

4. *July 24, WYFF 4 (SC)* — **All roads surrounding chemical plant shut down following explosions.** Owners of the Glo-Tex chemical plant in Spartanburg County, SC, said that they expected to be open for business on Monday, July 24. A fire on Friday caused multiple explosions and temporarily shut down all roads around the building.

Source: <http://www.wyff4.com/news/9560742/detail.html?rss=gs&psp=news>

5. *July 24, Statesman Journal (OR)* — **Streets blocked off following ammonia leak at Oregon plant.** Salem, OR, police and fire officials responded to a report Monday morning, July 24, of an ammonia leak coming from Deluxe Ice Cream on the 1800 block of State Street at 5:48 a.m. PDT. The leak was stopped at 6:30 a.m. PDT. One adult who was exposed to the fumes was

taken to Salem Hospital for evaluation. The area was blocked off for about one hour and 15 minutes. The ammonia, which is used as coolant, came from a leak in the refrigeration system.  
Source: [http://159.54.226.83/apps/pbcs.dll/article?AID=/20060724/UPD\\_ATE/60724002](http://159.54.226.83/apps/pbcs.dll/article?AID=/20060724/UPD_ATE/60724002)

[[Return to top](#)]

## **Defense Industrial Base Sector**

6. *July 24, Washington Technology* — **Defense transformation fires huge contract opportunities for IT security, networking, knowledge management, and outsourcing.** The Department of Defense's (DoD) drive to transform the way it does business is reflected in a spate of new information technology contracts valued from \$300 million to \$30 billion. An analysis for Washington Technology by market research firm Input Inc. identified 22 contracts that reflect the hottest opportunities in the coming months. Many of the contracts are "recompetes" or follow-ons to established contracts, and they reflect the growing use of omnibus procurement contracts. Big, multiple-award contracts give DoD the flexibility to quickly deal with emerging requirements by issuing task orders, while getting the good prices already negotiated under the contracts, said Michael Gaffney, president of business development for the federal sector at Computer Sciences Corp. DoD is backing away from using General Services Administration contracts and returning to military-specific contracts to get better results, said Ed Faulkner, group vice president and general manager of the defense systems group at Apogen Technologies Inc. of McLean, VA. The contracts also underscore DoD's focus on business transformation, IT security, interagency networking and knowledge management, and outsourcing.  
Input's list: <http://www.washingtontechnology.com/newspics/HotContracts2006.pdf>  
Source: [http://www.washingtontechnology.com/news/21\\_14/defense/28997-1.html](http://www.washingtontechnology.com/news/21_14/defense/28997-1.html)

7. *July 23, Chicago Tribune* — **Battle for U.S. defense work goes global.** The Franco-German company European Aeronautic Defense and Space Co. (EADS) last month won a helicopter contract from the U.S. Army potentially worth up to \$2 billion. EADS is also vying for a contract for a light cargo plane that the Army and Air Force envision as a versatile battlefield transport. And on the horizon is the biggest prize of all: A pact for hundreds of aerial refueling tankers to be delivered during the next two decades, pitting EADS, the parent company of European jetmaker Airbus SAS, against Chicago-based Boeing Co. The deals will test the nation's interest in foreign military suppliers in an increasingly global defense industry. Overseas defense contractors want a bigger piece of the American military budget, the largest in the world, but face opposition from national security critics who worry about jobs, technology, and secrets leaving the country. The Department of Defense supports an international supply base to create as much competition as possible.  
Source: <http://www.chicagotribune.com/business/chi-0607230299jul23.1.4126175.story?coll=chi-business-hed>

[[Return to top](#)]

## **Banking and Finance Sector**

8. *July 24, Register (UK)* — **Unsolicited credit card push irks security researchers.** A top UK security expert has criticized the practice of issuing unsolicited credit cards. Professor Ross Anderson of Cambridge University reports how his wife recently received a pre-approved, unsolicited Gold Mastercard from UK store Debenhams. Cutting up the card and throwing it in the bin simply doesn't pass muster, he argues. For one thing, the UK's move to Chip and PIN on plastic cards as an alternative to signature-authorized transactions complicates the problem of disposing of unwanted plastic cards. "The average customer has no idea how to 'cut up' a card now that it's got a chip in it," he writes. According to Anderson, bisecting the plastic using scissors leaves the chip functional.  
Anderson's statement: <http://www.lightbluetouchpaper.org/2006/07/20/new-card-security-problem/>  
Source: [http://www.theregister.co.uk/2006/07/24/unsolicited\\_credit\\_card\\_push/](http://www.theregister.co.uk/2006/07/24/unsolicited_credit_card_push/)
9. *July 24, Register (UK)* — **Warning over Sky TV scam.** Credit card scammers are targeting Sky TV subscribers with a new two-part scam. In the first part of the ruse, a pre-recorded telephone call asks members of the public if they subscribe to Sky TV. A week or so later, the prospective mark receives a telephone call from a scammer, posing as a Sky employee, claiming the customer's Sky subscription is unpaid and warning that their subscription will be suspended unless they make credit card payment. Those who fall for the ruse will find their credit card details in the hands of scammers, who can use the data to make fraudulent transactions.  
Source: [http://www.theregister.co.uk/2006/07/24/sky\\_tv\\_scam/](http://www.theregister.co.uk/2006/07/24/sky_tv_scam/)
10. *July 23, Washington Post* — **A new banking scam in Washington, DC.** The wig is the chic weapon du jour of one of the Washington, DC-area's most prolific and ingenious criminals. Police say the woman has walked into several banks in Montgomery County, MD, and the District of Columbia wearing wigs and other accessories to impersonate account holders. It works like this: She deposits a random check she has made out to the account holder and through that transaction obtains the victim's account number. Then, the same day or a day later, she uses fake or stolen identification and the victim's debit card, also stolen, to get the teller to process a withdrawal. By the time the original check bounces, she's long gone. Since September, the woman has used her extensive collection of wigs, scarves, headbands and hats to help her pilfer more than \$200,000 from the checking accounts of at least 20 women. Montgomery police Detective Brandon Mengedoht believes that the suspect is probably part of a sophisticated theft ring that includes pickpockets and document forgers.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/22/AR2006072200991.html>
11. *July 22, eWeek* — **Visa changes retail security rules.** Visa on Friday, July 21, changed its retail security requirement structure, which will — because of a change in definition of what a qualifying transaction is — force more retailers to use its more stringent security procedures. The core change includes all transactions when determining what level a retailer should be; Visa uses four levels to group retailers based on their volume of transactions. The criteria was previously limited to online purchases. "The most significant modification involves the Level 2 merchant category, which previously only applied to merchants processing between 150,000 and six million Visa e-commerce transactions per year," a Visa statement said. "Level 2 has now been broadened to include all acceptance channels and applies to any merchant processing

one million to six million Visa transactions per year."

Visa statement: [http://www.usa.visa.com/about\\_visa/newsroom/press\\_releases/n\\_r325.html](http://www.usa.visa.com/about_visa/newsroom/press_releases/n_r325.html)

Source: <http://www.eweek.com/article2/0.1895.1993067.00.asp>

12. *July 20, Websense Security Labs* — **Phishing Alert: UMB Financial Corporation.** Websense Security Labs has received reports of a new phishing attack that targets customers of UMB Financial Corporation. Users are given a link to a fraudulent Website, where they are prompted to enter their personal and financial details.  
Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=557>
13. *July 20, Websense Security Labs* — **Phishing Alert: University of Wisconsin Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of University of Wisconsin Credit Union. Users receive a spoofed e-mail claiming that, due to new security measures, the user must verify his or her account. The message provides a link to a phishing Website that asks for account and personal information.  
Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=556>
14. *July 20, Department of the Treasury* — **Treasury designates Canadian and Sudanese national for support to al Qaeda.** On Thursday, July 20, The Department of the Treasury designated Abu Sufian Al-Salamabi Muhammed Ahmed Abd Al-Razziq, a Canadian and Sudanese citizen, for his high-level ties to and support for the al Qaeda network. Thursday's designation of Abd Al-Razziq, carried out by the Treasury's Office of Foreign Assets Control, was executed under Executive Order 13224, an authority that targets the assets of terrorists and their financiers.  
Source: <http://www.treasury.gov/press/releases/hp22.htm>
15. *July 18, Department of the Treasury* — **Treasury adds two entities to the list of Iranian weapons proliferators.** The Department of the Treasury on Tuesday, July 18, designated two additional Iranian companies, Sanam Industrial Group and Ya Mahdi Industries Group, for their ties to missile proliferation. This action was taken pursuant to Executive Order 13382, an authority aimed at financially isolating proliferators of weapons of mass destruction (WMD), their supporters, and those contributing to the development of missiles capable of delivering WMD. Designations under Executive Order 13382, which is administered and enforced by the Treasury's Office of Foreign Assets Control, prohibits all transactions between the designees and any U.S. person and freezes any assets the designees may have under U.S. jurisdiction.  
Source: <http://www.treasury.gov/press/releases/hp17.htm>

[[Return to top](#)]

## **Transportation and Border Security Sector**

16. *July 24, Agence France-Presse* — **Anti-hijack software under development.** Some 30 European businesses and research institutes are working to create software that would make it possible from a distance to regain control of an aircraft from hijackers, according to the German news magazine, Der Spiegel. The system "which could only be controlled from the ground would conduct the aircraft posing a problem to the nearest airport whether it liked it or not,"

said the article. The project involves aircraft maker Airbus, electronics giant Siemens, and the Technical University of Munich. The first results should be presented in Britain in October, the magazine said.

Source: [http://news.yahoo.com/s/afp/20060722/tc\\_afp/germanyeeunrest:\\_ylt=Al7aXF7ZhgiC1477pY7qfsMjtBAF:\\_ylu=X3oDMTA0cDJlYmhvBHNIY\\_wM-](http://news.yahoo.com/s/afp/20060722/tc_afp/germanyeeunrest:_ylt=Al7aXF7ZhgiC1477pY7qfsMjtBAF:_ylu=X3oDMTA0cDJlYmhvBHNIY_wM-)

17. *July 24, Associated Press* — **Thousands re-screened after California airport security breach.** Both terminals at John Wayne Airport, 35 miles south of Los Angeles, were temporarily evacuated Sunday evening, July 23, and passengers were taken off airplanes after a female passenger made it past a security checkpoint without being screened, authorities said. Hundreds of travelers — even those aboard airplanes — were required to undergo a second security check, said Nico Melendez of the Transportation Security Administration. Six outgoing flights were delayed as passengers were re-screened and put back on the planes, Melendez said. An alarm sounded shortly after 5:30 p.m. PDT and Orange County Sheriff's deputies and airport security began evacuating the terminals. Lines snaked out the doors as travelers lined up again in front of checkpoints. Many passengers missed their flights and were forced to rebook on later flights.

Source: [http://www.usatoday.com/travel/news/2006-07-23-security-breach\\_x.htm](http://www.usatoday.com/travel/news/2006-07-23-security-breach_x.htm)

18. *July 24, Associated Press* — **Transit travel alerts keep commuters moving.** When storms knocked down a tree and damaged overhead power lines on NJ Transit tracks in suburban Montclair in the past week, it wasn't long before plugged-in commuters found out what that would mean for the next morning's rush hour. They got an alert from NJ Transit, which transmits messages to about 38,000 commuters via cell phone, hand-held computer and e-mail of service disruptions for their requested lines and times. The number of customers requesting the alerts jumped about 52 percent over the past year. Increasingly, transit agencies are embracing technology to make their customers' rides smoother and more predictable. Just as airline customers can sign up for alerts advising them of flight cancellations, transit agencies are using similar technology. Commuters around metro Seattle, Portland, and Cincinnati can enroll in customized e-mail alert programs to inform them of delays. Atlanta's MARTA system is considering a similar service, said Joselyn Baker, a spokesperson.

Source: <http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVEeXk1JmZnYmVsN2Y3dnFIZUVFeXk2OTY1NjJwJnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mg==>

19. *July 24, Associated Press* — **FBI joins investigation into deadly Indiana highway shootings.** The FBI has joined the investigation Monday, July 24, into the sniper shootings along two Indiana interstates that killed one person and wounded another, as police combed fields, overpasses, and roads for evidence. Investigators turned over bullets and other forensic evidence to the Indiana State Police crime lab to determine how many and what type of weapons were used in Sunday's shootings 100 miles apart, said state police Sgt. Jerry Goodin. Police have received more than a dozen calls through a tipline set up specifically for the shootings, state police Sgt. Rod Russell said Monday. Delaware County Sheriff George Sheridan said his department has added extra patrols and asked residents to call if they have information to share. Electronic signs along Indiana highways also urged people to come forward with anything strange they might have seen or heard. Police also have collected video surveillance tapes from businesses near the shooting sites. Indiana police also were consulting

with police from Columbus, Ohio. In late 2003 and early 2004, a sniper there killed one person in a series of random highway shootings.

Source: <http://www.pal-item.com/apps/pbcs.dll/article?AID=/20060724/NEWS01/60724005>

20. *July 24, San Francisco Chronicle* — **Surveillance via software helps airport.** In the Security Operations Center at San Francisco International Airport, a technician watches a dozen monitors fed by the 1,500 surveillance cameras scattered through the sensitive facility. At the far right sits the newest tool in the airport's security toolkit — a computer monitor that displays images, selected by a new type of software, that sifts through that stream of surveillance video, sending out alerts when it detects certain actions or situations. The software being evaluated represents an emerging technology called video analytics. The idea is to use software algorithms to scan surveillance video gathered by closed circuit television cameras and to search for specific visual patterns — such as two airport workers scooting through a security door at the same time, when they should enter one at a time, or a vehicle parked too long at a place where it shouldn't be. Jason Halverson, a security industry analyst with Frost & Sullivan in San Antonio, said these programs try to make better use of all the surveillance video that is currently captured giving security officials a better chance to thwart danger. Security experts say video analytics has been spurred by advances in computer technologies, and by reaction to terrorist attacks.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/24/BUGEHK1UA21.DTL>

21. *July 23, Associated Press* — **Las Vegas flight quarantined.** A section of the airport at Las Vegas, NV, was closed for several hours after a flight arrived from Denver with 11 sick people on board, officials said Sunday, July 23. Passengers and crewmembers on United Airlines Flight 1491 were quarantined for several hours Saturday night, July 22, at McCarran International Airport while the plane, passengers and luggage were checked by hazardous materials experts, said Elaine Sanchez, a McCarran spokesperson. Sanchez said the cause was still being investigated. A passenger, Don Yarbrough, said that investigators believed the victims reacted to a cleaning fluid containing ammonia that had been used on the plane after it arrived in Denver from Cancun, Mexico.

Source: [http://www.usatoday.com/travel/flights/2006-07-23-flight-quarantine\\_x.htm](http://www.usatoday.com/travel/flights/2006-07-23-flight-quarantine_x.htm)

22. *July 20, Pacific Business News* — **AMR orders more than 100 winglets.** Winglets — those upturned fins on the edges of Aloha Airlines jet wings — are going to be a lot more common on American Airlines jets as well. American parent company AMR Corp. confirmed Wednesday, July 19, that after ordering 20 winglets installed on Boeing 757-200s a year ago, it has ordered another 104 winglet shipsets. Winglets reduce fuel consumption by up to 200,000 gallons per plane per year.

Source: <http://biz.yahoo.com/bizj/060720/1318019.html?.v=2>

[[Return to top](#)]

## **Postal and Shipping Sector**

Nothing to report.

[[Return to top](#)]

## **Agriculture Sector**

**23. *July 24, Ohio Ag Connection* — Ash borer quarantine expanded in Ohio.** Ohio Department of Agriculture Director Fred Dailey Friday, July 21, announced the expansion of the Emerald Ash Borer (EAB) quarantine in central Ohio. The quarantine, which now encompasses the northeast corner of Franklin County, halts the movement of ash tree material and firewood and the continued spread of the ash tree-killing insect. In Franklin County, the department has now quarantined the area within the boundaries of Interstate Highway 71 to Interstate Highway 70 to the Licking and Delaware County borders. It is illegal to move ash trees, parts of ash trees, and all hardwood firewood out of the newly quarantined area. "We have been intensively surveying the area to better assess the infestation in Franklin County," Dailey said. "At this point, we have discovered several other infested trees and have expanded the quarantined area to keep the pest where we know it exists." Franklin County is one of 15 counties, or parts within, quarantined in northwest and central Ohio. Additional counties include Auglaize, Defiance, Delaware, Erie, Fulton, Hancock, Henry, Huron, Lorain, Lucas, Sandusky, Ottawa, Wood, and Williams. Quarantines also prohibit the movement of regulated material into Ohio from Michigan and parts of Indiana.

EAB information: <http://www.emeraldashborer.info/>

Source: [http://www.ohioagconnection.com/story-state.cfm?Id=460&yr=20\\_06](http://www.ohioagconnection.com/story-state.cfm?Id=460&yr=20_06)

**24. *July 24, Grand Forks Herald (ND)* — Missing cattle in South Dakota.** Rustlers are suspected in the disappearance of 88 head of cattle in Aurora and Douglas counties in South Dakota. The cattle, worth around \$43,000, were taken from two remote rural farms about 15 miles apart. Fifty Holstein steers weighing 250 to 400 pounds each were taken from one location, and 38 Holstein steers weighing about 500 pounds each were taken from another, according to authorities. Aurora County Sheriff David Fink said cattle disappearances in the past haven't involved such large numbers.

Source: <http://www.grandforks.com/mld/grandforks/news/15107896.htm>

**25. *July 19, Associated Press* — Iowa's veterinary response team grows.** The Iowa Veterinary Rapid Response Team (IVRRT), a nearly all-volunteer force, is growing quickly as this Midwestern state prepares for possible incidents of foreign animal disease, agroterrorism and large scale natural disasters, state homeland security officials said Wednesday, July 19. The teams are responsible for animal disease surveillance and diagnosis, as well as for control and eradication of diseases. Their activities may include quarantining animals, prohibiting animal movement, disinfecting farms, euthanizing animals and planning for carcass disposal. The IVRRT, which works with the Iowa Department of Public Health, the U.S. Department of Agriculture and other state and federal partners, is overseen by the state veterinarian and secretary of agriculture. The team gets its authority from the Legislature. Last year, the team had its first response so far. It set up a treatment center at the Iowa State Fairgrounds to help assist pets of Hurricane Katrina evacuees, after many of the 600 families brought their companion animals along with them to Iowa.

Iowa Veterinary Rapid Response Team: <http://www.agriculture.state.ia.us/IVRRT.htm>

Source: <http://www.heraldnewsdaily.com/stories/news-00204774.html>

[[Return to top](#)]

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

**26. *July 24, Reuters* — Arabs need to spend \$100 billion on water by 2016.** Arab states will need to invest a \$100 billion on desalination over the next decade if demand for water keeps growing at the current pace, especially in the Gulf region, an energy services firm said on Saturday, July 22. The firm said industry data showed that demand for desalinated water in the Arab world was growing at an annual average of six percent, double the global average. The firm said rapid economic growth in Dubai, commercial hub of the arid Gulf region, was putting an unprecedented strain on the emirates energy and water resources. Demand for water in Dubai during the peak summer season rose 10 percent to touch 184 million gallons per day in 2004, according to the latest available figures.

Source: [http://today.reuters.co.uk/news/newsArticle.aspx?type=scienc&News&storyID=2006-07-24T125821Z\\_01\\_L22866375\\_RTRIDST\\_0\\_SCIE\\_NCE-UTILITIES-WATER-ARABS-DC.XML](http://today.reuters.co.uk/news/newsArticle.aspx?type=scienc&News&storyID=2006-07-24T125821Z_01_L22866375_RTRIDST_0_SCIE_NCE-UTILITIES-WATER-ARABS-DC.XML)

**27. *July 23, Associated Press* — Drought worsens across nation.** The drought gripping much of the nation is expanding in both size and severity, the National Drought Mitigation Center at the University of Nebraska–Lincoln said. The areas most affected by the drought stretch from Georgia to Arizona. But areas of severe drought are growing in the Upper Midwest. The hardest-hit spot covers central South Dakota and reaches into southern North Dakota, according to a drought map updated weekly by the center. Iowa is about 3.42 inches short of its normal precipitation for January 1 to July 21.

National Drought Mitigation Center: <http://drought.unl.edu/>

Source: <http://www.grandforks.com/mld/grandforks/news/15106325.htm>

[\[Return to top\]](#)

## **Public Health Sector**

**28. *July 24, Reuters* — Fake malaria drugs threatening Africa.** Fake China-made malaria drugs, which have flooded parts of Asia and killed many people in recent years, are beginning to show up in Africa where the dummy tablets are expected to take far more lives, a World Health Organization (WHO) expert has warned. Malaria kills 1.3 million to three million people a year, and 90 percent of them occur in Africa. Since 2001, the WHO has recommended therapies containing artesunate, a compound extracted from a Chinese herb. But fake artesunate has flooded places such as Cambodia, Laos Vietnam and Myanmar in recent years, resulting in deaths. Kevin Palmer, WHO's regional adviser for malaria in the western pacific, said "they are also showing up in Africa, this is what we are worried about ... there is a massive market there and the malaria there is very serious so we are going to find more people who are really being killed or harmed by these drugs." Factories in China's southwestern Guilin city churn out the genuine drug, but there are at least 12 different types of copies – with either too little artesunate

to be helpful or none at all — that have been traced back to China.

Source: [http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006-07-24T121103Z\\_01\\_T21758\\_RTRIDST\\_0\\_HEALTH-MALARIA-DC.XML&archived=False](http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006-07-24T121103Z_01_T21758_RTRIDST_0_HEALTH-MALARIA-DC.XML&archived=False)

29. *July 23, Agence France-Presse* — **Simulations key to Asia's bird flu preparedness.** Asia Pacific nations should carry out regular exercises to test their preparedness for a bird flu pandemic, communicable disease experts said after witnessing a simulation in Singapore. Countries remain vulnerable because little is known about the bird flu virus and a vaccine has yet to be developed. But casualties can be minimized if governments are ready, said the experts who observed the two-day exercise which ended Saturday, July 22, in the city-state. One of the challenges facing the region is uncertainty over what happens in a pandemic, said Ancia Anne, regional inter-agency coordinator on avian and human influenza at the United Nations Development Program.

Source: [http://news.yahoo.com/s/afp/20060723/hl\\_afp/healthflusingapore\\_060723215930;\\_ylt=AktTN82ZI7Oz1GpRCqYkJamJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060723/hl_afp/healthflusingapore_060723215930;_ylt=AktTN82ZI7Oz1GpRCqYkJamJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

[[Return to top](#)]

## **Government Sector**

Nothing to report.

[[Return to top](#)]

## **Emergency Services Sector**

30. *July 23, Today's Sunbeam (NJ)* — **Emergency drill launched to test response in New Jersey county.** In an effort to test the Salem County, NJ, ability to respond to terrorist attacks, county leaders and emergency personnel worked through realistic scenarios on Saturday, July 22 in a table top emergency response meeting. The six-hour drill, held at the Salem County Emergency Management Building, was attended by over 80 emergency responders from the county and state levels who were called on to respond to three realistically simulated terrorist attacks that occurred within minutes of each other in different areas of the county. "We felt it was important for the county to have this type of drill that involved all areas to evaluate the county and individual municipality's ability to handle multiple major terrorist attacks on a simultaneous basis," Salem County Prosecutor John Lenahan said. Through the exercise, county personnel learned of several improvements that need to be made in the county's emergency response procedures including the need for more hospital space for attack victims and the need to improve upon the decontamination facilities that are currently available. Lenahan said they plan on holding other exercises in the future including real world training where they will send emergency personnel out to accident scenes.

Source: <http://www.nj.com/news/sunbeam/local/index.ssf?/base/news-1/1153635177268680.xml&coll=9>

31.

*July 22, Clanton Advertiser (AL)* — **County E-911 tower struck by lightning.** An E-911 tower took a hit from lightning in Chilton County, AL, on Friday, July 21 as thunderstorms swept through the area. Chilton County Emergency Management Agency Director Bill Collum said the county might look at setting up an alternate site elsewhere in the county so that if one tower was knocked out, there would be a backup tower. "We built redundancy into that system last year by adding a lot of radios, but we're still operating off of that one tower," Collum added. "We might want to set up at a different location." Even without an operating communications tower, county first responders were able to effectively communicate with each other.

Source: <http://www.clantonadvertiser.com/articles/2006/07/22/news/a- news.txt>

32. *July 22, Daily Citizen (AR)* — **Long distance fees for 911 calls in Arkansas city questioned.** Phone companies are charging long distance fees for 911 calls transferred outside of the Searcy, AR, calling area, a policy that is costing taxpayers. While a 911 caller does not pay a long distance fee to contact the 911 emergency dispatch center located in Searcy, the dispatch center itself is billed for calls made to police, fire departments or ambulance services if they are long distance. Tamara Jenkins, 911 Coordinator, brought the extra billing to the attention of the White County 911 Emergency Services Administrative Board. "As long as they're on the line talking them through the emergency, we get charged," J.R. Thomas, Chairman of the 911 Board, said. "We stay on the line to see if they are going to need additional backup," Jenkins said. "We can be on the line from two minutes to 30 minutes, depending on the type of call." Every time 911 is called from outside the Searcy calling area, the 911 dispatch center pays the long distance fees. The board plans to have phone company representatives meet with them to explain the extra fees. Meanwhile, the charges still pile up, costing thousands of dollars over the course of a year.

Source: <http://www.thedailycitizen.com/articles/2006/07/23/news/local news/news01.txt>

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

33. *July 24, IDG News Service* — **Microsoft offers second beta of Exchange Server 2007.**

Microsoft has released a new beta version of Exchange Server 2007 and the beta for an accompanying antivirus product, Forefront Security for Exchange, it announced on Monday, July 24. The second beta of Exchange Server 2007 is a "full-featured" release that's more reliable than the previous version and adds new management and mobility features, Microsoft said. The full product will be released late this year or early in 2007, the company said.

The beta can be downloaded at: <http://www.microsoft.com/exchange/beta2>

Source: [http://www.infoworld.com/article/06/07/24/HNexchangeserverbeta\\_1.html](http://www.infoworld.com/article/06/07/24/HNexchangeserverbeta_1.html)

34. *July 24, Associated Press* — **AMD to buy chip maker ATI for \$5.4 billion.** Advanced Micro Devices Inc. (AMD) said Monday, July 24, it will pay \$5.4 billion to acquire top graphics chip maker ATI Technologies Inc., as Intel Corp.'s biggest rival in the market for personal-computer microprocessors attempts to expand its product portfolio. The AMD-ATI marriage could shift the balance of power in the chip industry in significant ways. AMD's product portfolio — which has remained limited to the microprocessors that act as a PC's main calculating engine — would balloon overnight, as it folds in two major new chip categories.

Source: [http://news.yahoo.com/s/ap/20060724/ap\\_on\\_hi\\_te/amd\\_acquisit ion: ylt=AkULSEFb00894gDULMjgEwYjtBAF; ylu=X3oDMTA2Z2szazkxB HNIYwN0bQ--](http://news.yahoo.com/s/ap/20060724/ap_on_hi_te/amd_acquisit ion: ylt=AkULSEFb00894gDULMjgEwYjtBAF; ylu=X3oDMTA2Z2szazkxB HNIYwN0bQ--)

35. *July 21, Information Week* — **UBS trial aftermath: Even great security can't protect you from the insider.** The recent UBS PaineWebber computer sabotage trial is a perfect example of the damage that can be caused by a knowledgeable insider with high-level access and an axe to grind. A company employee is already inside the perimeter, where the vast majority of the protective technologies sit. That same employee also knows what information is most vital to the company's ability to make money and sustain itself. He has knowledge of passwords, and he also probably knows what kind of machines and operating systems the company is running. An IT professional has all this information, plus he has access to the inner workings of the infrastructure. He has high-level privileges that allow him access to key servers and databases, and possibly even root-level access, which would give him all-encompassing power over the system. UBS PaineWebber's network was hit by a logic bomb in March of 2004. A jury last week found Roger Duronio of Bogota, NJ, guilty of two crimes: computer sabotage for building, planting and distributing the malicious code that brought down nearly 2,000 servers on the company's nation-wide trading network; and securities fraud.

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=DY4LHGUFJWTSEQSNDLPSKHSCJUNN2JVN?articleID=191000063>

36. *July 21, Federal Computer Week* — **DHS authorization bill: A mandate for info sharing.** The Department of Homeland Security (DHS) has had information sharing on its list of technology must-dos for some time, but it would become a mandate under the fiscal 2007 authorization bill a House panel recently passed. In the bill it cleared Wednesday, July 19, the House Homeland Security Committee called on DHS' secretary to establish a comprehensive information technology network architecture to be run by the renamed Office of Intelligence and Analysis. The new office would oversee intelligence sharing among DHS' various intelligence agencies, and information-sharing and knowledge officers would run the office's activities.

Source: <http://www.fcw.com/article95373-07-21-06-Web>

37. *July 21, ZDNet News* — **BellSouth shareholders approve AT&T merger.** Despite opposition from consumer and advocacy groups, BellSouth shareholders have given the green light to the company's \$67 billion merger with AT&T. The merger, announced in March, would create a telecommunications giant that dwarfs its nearest competitor, Verizon Communications.

Source: [http://news.zdnet.com/2100-9595\\_22-6097110.html](http://news.zdnet.com/2100-9595_22-6097110.html)

38. *July 20, Secunia* — **Sun Solaris event port API denial-of-service vulnerability.** Some vulnerabilities have been reported in Solaris, which can be exploited to cause a denial-of-service. Analysis: The vulnerabilities are caused due to unspecified errors in the event port API and can be exploited by malicious, local users to run an application using the API in such a way that the system crashes. On systems running e.g. Apache2, it may be possible for malicious people to crash the system (the Apache2 Web server distributed with Solaris 10 in the SUNWapch2d and SUNWapch2u packages is, however, not affected). Vulnerable: Sun Solaris 10.

Solution: Apply patches: SPARC Platform: Solaris 10: Apply patch 118833-12 or later.

x86 Platform: Solaris 10: Apply patch 118855–10 or later.

Original Advisory: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102485-1>

Source: <http://secunia.com/advisories/21132/>

- 39. July 20, Security Focus — Flaw finders lay siege to Microsoft Office.** Responding to a steady influx of flaws in the company's Office productivity suite has occupied many of Microsoft's programmers since late 2005. So far this year, the software giant has detailed at least 24 Office flaws found by outside researchers in its monthly bulletins, six times the number of Office flaws found in all of 2005. The count also surpasses the 20 flaws that Microsoft has fixed so far this year in Internet Explorer, a perennial favorite among vulnerability researchers. The extraordinary jump in the number of flaws discovered by researchers in the components of Office has worried system administrators and forced Microsoft to spend development time on fixing the issues. The deluge of vulnerabilities for the Office programs signals a shift in the focus of vulnerability research and underscores the impact of flaw-finding tools known as fuzzers. The vulnerabilities in Office also highlight the threat that such files, if remained unchecked, can pose to a corporate network. The focus on Office flaws is a microcosm of the overall shift among vulnerability researchers from network service and server flaws to the application flaws that can be exploited to compromise a user's PC.

Source: <http://www.securityfocus.com/news/11401>

### Internet Alert Dashboard

#### DHS/US–CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US–CERT Operations Center Synopsis:** US–CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

**VU#936945:** Microsoft PowerPoint contains an unspecified remote code execution vulnerability. <http://www.kb.cert.org/vuls/id/936945>

US–CERT strongly recommends the following until an update, patch, or more information becomes available:

Do not open attachments from unsolicited email messages.

Install anti virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments. <http://www.us-cert.gov/cas/tips/ST04-010.html>

US-CERT will continue to update current activity as more information becomes available.

## **PHISHING SCAMS**

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

### **Current Port Attacks**

<b>Top 10 Target Ports</b>	44139 (—), 1026 (win-rpc), 4672 (eMule), 38566 (—), 445 (microsoft-ds), 24232 (—), 80 (www), 25 (smtp), 65530 (WindowsMite), 113 (auth) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.